Password Policy (Client User)

All WJPS software Users are supplied with a system-generated password when they are added to the system. Please ensure you follow the below password security guidelines:

- Any initial system-generated passwords or those set by IT personnel in an organisation must be changed the first time they are used by the user.
- Passwords should be no less than 8 characters in length and consist of both numbers and letters.
- Passwords MUST NOT be written down either on paper or retained electronically, (unless the Client User is using secure password manager software to store passwords). If the password is written down at any point the paper must be destroyed as soon as possible.
- Passwords must be kept confidential and not be shared or given to anyone else within a user's organisation.